
	<b>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información</b>	CÓDIGO: PL3_TIC
		VERSIÓN: 2
	<b>Direccionamiento Estratégico</b>	FECHA DE APROBACION: 29/01/2026
		Página: 1 de 8

## TABLA DE CONTENIDO

INTRODUCCIÓN .....	2
1. OBJETIVO .....	3
2. ALCANCE .....	3
3. DEFINICIONES .....	3
4. NORMATIVIDAD ASOCIADA .....	3
5. DESARROLLO .....	5
<b>Identificación</b> .....	6
<b>Evaluación de riesgos</b> .....	6
<b>Mitigación y tratamiento de riesgos</b> .....	6
<b>Monitoreo y revisión continua</b> .....	6
<b>Estrategia de Implementación</b> .....	6
6. DOCUMENTOS DE REFERENCIA .....	8
7. RELACIÓN DE FORMATOS .....	8
8. CONTROL DE CAMBIOS .....	8

	<b>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información</b>	<b>CÓDIGO: PL3_TIC</b>
		<b>VERSIÓN: 2</b>
	<b>Direccionamiento Estratégico</b>	<b>FECHA DE APROBACION: 29/01/2026</b>
		<b>Página: 2 de 8</b>

## INTRODUCCIÓN

En la actualidad, la gestión de la seguridad y privacidad de la información es un elemento crítico para el éxito y la sostenibilidad de cualquier organización. Este plan de tratamiento de riesgos ha sido diseñado con el objetivo de abordar de manera efectiva los riesgos asociados a la seguridad y privacidad de la información, siguiendo las directrices establecidas en el Modelo de Seguridad y Privacidad de la Información (MSPI) y la política de gestión de riesgos de nuestra organización.

La adopción de este plan nos permitirá identificar, evaluar y gestionar los riesgos de manera proactiva, asegurando así la integridad, confidencialidad y disponibilidad de nuestra información crítica. Es un enfoque integral que no solo abarca los aspectos tecnológicos, sino también los procesos organizativos y el factor humano.

A continuación, se ilustra en que acciones del MSPSI se tendrá interacción directa con el Modelo de Gestión de Riesgos de Seguridad de la información:

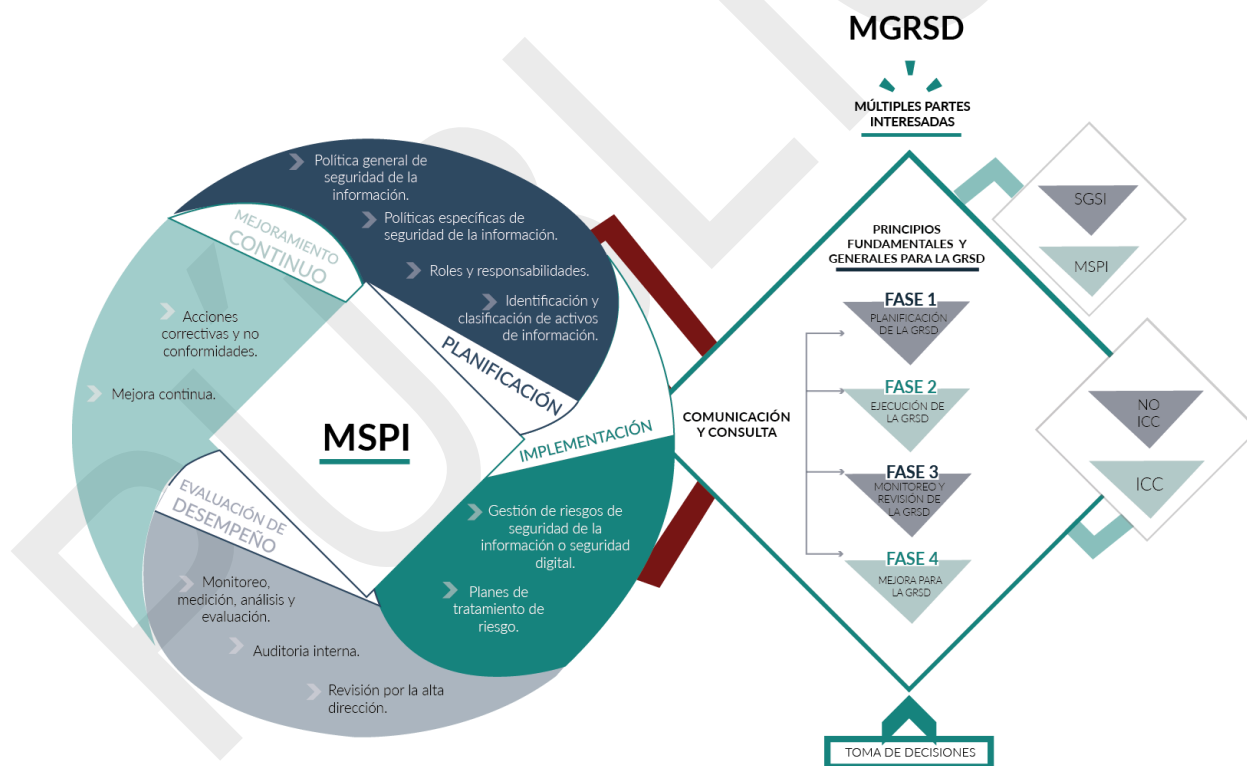



Ilustración 1. Fuente: MinTic.

	<b>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información</b>	CÓDIGO: PL3_TIC
		VERSIÓN: 2
	<b>Direccionamiento Estratégico</b>	FECHA DE APROBACION: 29/01/2026
		Página: 3 de 8

## 1. OBJETIVO

Definir y aplicar los lineamientos para la gestión de riesgos de seguridad de la información y seguridad digital que permita preservar la integridad, confidencialidad y disponibilidad de la información institucional.

## 2. ALCANCE

Este documento es aplicable para todas las gerencias, subgerencias u oficinas pertenecientes a la Entidad, por tal motivo en su ciclo de ejecución se involucran todos los procesos.

## 3. DEFINICIONES


- **Control de Seguridad:** Medidas implementadas para mitigar riesgos, proteger activos de información y garantizar el cumplimiento normativo.
- **Criptografía:** Técnica utilizada para proteger la información mediante el uso de algoritmos de cifrado, asegurando su confidencialidad e integridad.
- **Gestión de Cambios:** Proceso para asegurar que las modificaciones en los sistemas de información se realizan de manera controlada, minimizando impactos negativos.
- **Vulnerabilidad:** Debilidad en un activo de información o en las medidas de seguridad que puede ser explotada por una amenaza

## 4. NORMATIVIDAD ASOCIADA

Normatividad	Entidad	Descripción
Guía para la Gestión Integral del Riesgo en Entidades Públicas V7	Departamento Administrativo de la Función Pública	Guía para la Gestión Integral del Riesgo en Entidades Públicas
Acuerdo 002 de 2023	Comisión Distrital de Transformación Digital	Por la cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad.
Resolución 460 de 2022	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno digital, y se dictan los lineamientos generales para su implementación.
Resolución 500 de 2021	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Resolución 02277 de 2025	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

**Piensa en el medio ambiente, antes de imprimir este documento.**


Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	<b>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información</b>	CÓDIGO: PL3_TIC
		VERSIÓN: 2
	<b>Direccionamiento Estratégico</b>	FECHA DE APROBACION: 29/01/2026
		Página: 4 de 8

Normatividad	Entidad	Descripción
Decreto 620 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Resolución 1519 de 2020.	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos
Resolución 2893 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPA, y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado colombiano, y se dictan otras disposiciones
Directiva 002 de 2020	Presidencia de la Republica	Medidas para atender la contingencia generada por el covid-19, a partir uso de las tecnologías la información y las telecomunicaciones - TIC
CONPES 3995 de 2020.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política Nacional de Confianza y Seguridad Digital.
Decreto 612 de 2018	Presidencia de la Republica	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado
CONPES 3854 de 2016.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política de Seguridad Digital del Estado Colombiano
Decreto 1078 de 2015	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Ley 1712 de 2014	Presidencia de la Republica	Ley de transparencia y el derecho a la información pública nacional
Ley 1581 de 2012	Congreso de Colombia	Se dictan disposiciones generales para la protección de datos personales
CONPES 3701 de 2011.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Lineamientos de Política para Ciberseguridad y Ciberdefensa.

**Piensa en el medio ambiente, antes de imprimir este documento.**

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	<b>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información</b>	<b>CÓDIGO: PL3_TIC</b>
		<b>VERSIÓN: 2</b>
	<b>Direccionamiento Estratégico</b>	<b>FECHA DE APROBACION: 29/01/2026</b>
		<b>Página: 5 de 8</b>

## 5. DESARROLLO

Este documento detalla las actividades a implementar para la gestión de riesgos de seguridad de la información conforme las metodologías adoptadas por la entidad, las cuales se fundamenta en dos guías esenciales: la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" del Departamento Administrativo de la Función Pública (DAFP), en su versión más reciente de noviembre de 2022, y la "Guía de orientación para la gestión de riesgos de seguridad digital" del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Las fases para implementar incorporadas en el plan de gestión de riesgos están estrechamente alineadas con la Política de Administración de Riesgos y la Guía Administración de Riesgos de la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea". Esta alineación abarca desde la integración estratégica en la identificación de los riesgos de seguridad digital, hasta la implementación y seguimiento efectivo de las acciones para la gestión de riesgos institucionales.

El enfoque adoptado asegura una gestión de riesgos coherente y eficaz, cumpliendo con los estándares y recomendaciones establecidos tanto por el DAFP como por el MinTIC. Así, garantizamos que los riesgos de seguridad de la información sean identificados, evaluados y gestionados de manera integral, con un enfoque que promueve la mejora continua y la adaptación a los cambiantes entornos tecnológicos y de seguridad digital.

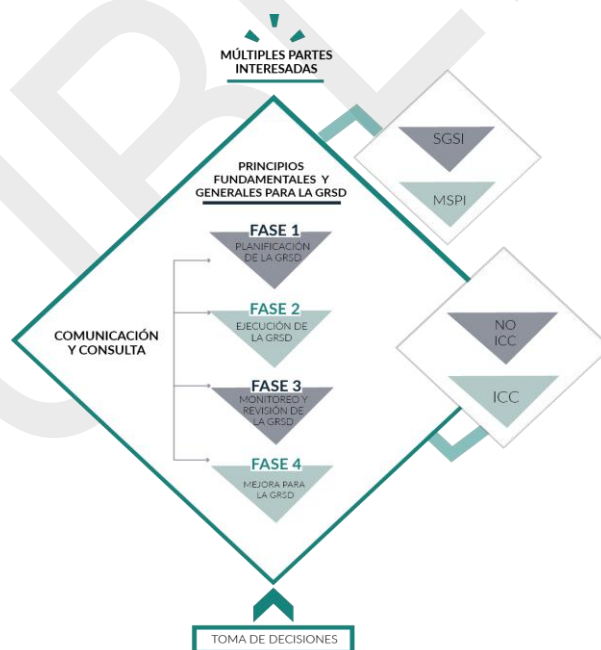



Ilustración 2. Marco conceptual de gestión del riesgo de seguridad digital Fuente: MinTic.

	<b>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información</b>	CÓDIGO: PL3_TIC
		VERSIÓN: 2
	<b>Direccionamiento Estratégico</b>	FECHA DE APROBACION: 29/01/2026
		Página: 6 de 8

## Identificación

Esta etapa implica el reconocimiento y la documentación de los riesgos potenciales que pueden impactar la seguridad de la información en la entidad. Siguiendo las directrices de las guías mencionadas, se debe realizar un mapeo detallado de los activos de información con criticidad alta, identificar las amenazas y vulnerabilidades asociadas a estos activos, y considerar tanto factores internos como externos que puedan influir en la seguridad de la información

## Evaluación de riesgos

Una vez identificados los riesgos, se procede a su evaluación, empleando un enfoque tanto cualitativo como cuantitativo. Esto implica determinar la probabilidad de ocurrencia de cada riesgo y su impacto potencial, en caso de materializarse.

La evaluación de riesgos se realiza considerando el contexto de la entidad y los criterios de valoración de riesgos establecidos, lo que permite priorizar los riesgos y tomar decisiones informadas sobre su tratamiento.

## Mitigación y tratamiento de riesgos

Basándose en la evaluación realizada, se desarrollan e implementan estrategias para manejar los riesgos. Esto puede incluir la reducción del riesgo mediante la implementación de controles, la transferencia del riesgo a través de seguros o contratos, la aceptación del riesgo cuando su impacto es tolerable, o la evitación del riesgo.

Las estrategias de tratamiento deben ser alineadas con los objetivos de la entidad y la eficiencia en el uso de los recursos.


## Monitoreo y revisión continua

La gestión de riesgos es un proceso dinámico, por lo que requiere un monitoreo y revisión constantes. Esto asegura que las estrategias de tratamiento de riesgos sigan siendo efectivas y pertinentes frente a cambios en el entorno interno o externo de la entidad.

Esta fase incluye la supervisión de los controles implementados, la revisión periódica del contexto de riesgo y la actualización de la evaluación de riesgos, así como la documentación y comunicación de los hallazgos pertinentes a las partes interesadas.


## Estrategia de Implementación

Para la vigencia 2026, se ejecutarán las siguientes actividades de acuerdo con el ciclo de gestión de los riesgos.

	<b>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información</b>	CÓDIGO: PL3_TIC
		VERSIÓN: 2
	<b>Direccionamiento Estratégico</b>	FECHA DE APROBACION: 29/01/2026
		Página: 7 de 8

Actividades	Entregable	Responsable	Finalización
Definir y aprobar la metodología y los criterios para la gestión del riesgo digital institucional, articulados con el DAFP	Guía Administración de Riesgos Atenea actualizada	Subgerente TICS  Contratista Profesional Ingeniero Seguridad de la información	16-01-2026
Identificar, analizar y evaluar riesgos de seguridad y privacidad asociados a los activos de información de mayor criticidad	Matriz de riesgos actualizada	Contratista Profesional Ingeniero Seguridad de la información / Líderes de proceso	31-05-2026
Establecer y aprobar planes de tratamiento del riesgo digital, con responsables y evidencias asignadas	Plan de tratamiento del riesgo	Líderes de proceso	30-06-2026
Realizar análisis de vulnerabilidades sobre infraestructura y servicios críticos	Informe técnico con hallazgos Elaborar y presentar el informe final de las acciones y vulnerabilidades encontradas	Contratista Profesional Ingeniero Seguridad de la información	Semestral
Realizar pruebas de restauración contempladas en el DRP/	Informe y evidencias de prueba	Contratista ingeniero de infraestructura	30-10-2026
Actualizar la Matriz de Aplicabilidad (SoA) del MSPI	Matriz actualizada	Contratista Profesional Ingeniero Seguridad de la información	31-03-2026
Actualizar y socializar el procedimiento de gestión y notificación de incidentes de seguridad digital, conforme a lineamientos del CSIRT Gubernamental y MSPI	Procedimiento oficial actualizado y evidencia de socialización	Contratista Profesional Ingeniero Seguridad de la información	30-04-2026
Desarrollo y verificación de codificación segura en aplicaciones institucionales	Documento con la validación ejecutada	Subgerencia TICS	15-12-2026



	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	CÓDIGO: PL3_TIC
		VERSIÓN: 2
	Direccionamiento Estratégico	FECHA DE APROBACION: 29/01/2026
		Página: 8 de 8

6. **ANEXOS:** No aplica

## 7. DOCUMENTOS DE REFERENCIA

- Guía para la Gestión Integral del riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública (DAFP). Versión 7, 2025
- Guía de orientación para la gestión de riesgos de seguridad digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Política Integral de riesgos -Atenea

## 8. RELACIÓN DE FORMATOS

CODIGO	NOMBRE DEL FORMATO
No aplica	No aplica

## 9. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
31/01/2025	PL3_TIC V1	Se ajusta el plan conforme a la actualización de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7 2025.

VALIDACIÓN	NOMBRE	CARGO	FECHA
<b>Elaboró</b>	Maria Alejandra Suarez Rojas	Contratista Profesional– Subgerencia Tecnologías de la información y las comunicaciones	29/01/2026
<b>Revisó</b>	Carlos Andrés Ballesteros Juan Pablo Ceballos	Subgerente Tecnologías de la información y las comunicaciones Contratista Profesional– Subgerencia Tecnologías de la información y las comunicaciones	29/01/2026
<b>Aprobó</b>	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño	29/01/2026

<b>NOMBRE Y FIRMA DEL LÍDER DE PROCESO</b>